The opinion in support of the decision being entered today was *not* written for publication and is *not* binding precedent of the Board.

UNITED STATES PATENT AND TRADEMARK OFFICE

BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Ex parte CAROLYN RAMSEY CATAN

Appeal 2007-0820
Application 09/734,808
Technology Center 1700

Decided: July 3, 2007

Before MICHAEL R. FLEMING, *Chief Administrative Patent Judge*, HUBERT C. LORIN, ALLEN R. MacDONALD, LINDA E. HORNER, and ANTON W. FETTING, *Administrative Patent Judges*.

PER CURIAM

DECISION ON APPEAL

STATEMENT OF THE CASE

The appeal is from a decision of the Examiner rejecting claims 5-11 and 13-16[1]. 35 U.S.C. § 134 (2002). We have jurisdiction under 35 U.S.C. § 6(b) (2002).

[1] Claims 1-4, 12, and 17 have been canceled.

Claims 5-11 and 13-16 are rejected under 35 U.S.C. § 103(a) (2002) over Nakano (US Patent 5,845,260) in view of Dethloff (US Patent 4,837,422) and Harada (US Patent 5,721,583).

We AFFIRM.

Appellant's claimed invention is a consumer electronics device using bioauthentication to authorize sub-users of an authorized credit account to place orders over a communication network up to a pre-set maximum sub-credit limit. The device includes a bioauthentication device, such as a fingerprint sensor (claim 6) or voice sensor (claim 8). The claimed electronics device comprises a memory, a processor, and a communications link. The memory stores account information for an account holder as well as bioauthentication information and sub-credit limits for authorized users of the account. The processor (a) detects a match between bioauthentication information received from the bioauthentication device and bioauthentication information stored in memory, and when a match is detected, (b) finds a sub-credit limit associated with the bioauthentication information, and when a sub-credit limit is not exceeded, (c) sends account holder information over the communication link to enable the user of the electronics device to place an order.

Appellant, in the Brief[2], argues claims 5-11 and 13-16 as a group. The Board selects representative claim 5 to decide the appeal. 37 C.F.R. § 41.37(c)(1)(vii) (2006). Accordingly, the remaining claims stand or fall with claim 5.

[2] Our decision will make reference to Appellant's Appeal Brief ("Appeal Br.," filed Aug. 9, 2006), the Examiner's Answer ("Answer," mailed Aug. 17, 2006), and to the Reply Brief ("Reply Br.," filed Oct. 17, 2006).

Claim 5 reads as follows:

> 5. A consumer electronics device, comprising
> a memory which stores account information for an account holder and sub-credit limits and bioauthentication information for authorized users of the account;
> a bioauthentication device which provides bioauthentication information to the memory;
> a communication link; and
> a processor, which compares received bioauthentication information to stored bioauthentication information to detect a match, and finds an associated sub-credit limit corresponding to the received bioauthentication information, to enable a purchase over the response network via the communication network up to a maximum of the sub-credit limit, the processor sending the account holder information over the communication link only if the match is detected and the sub-credit limit is not exceeded.

ISSUE

The issue is whether Appellant has shown that the Examiner erred in holding the combination of Nakano's consumer electronics device and Dethloff's and Harada's bioauthentication means would have rendered the subject matter of claim 5 obvious to one of ordinary skill in the art at the time of the invention.

FINDINGS OF FACT

The record supports the following findings of fact (FF) by a preponderance of the evidence.

1. Claim 5 does not describe the "consumer electronics device" of the preamble in terms that limit any function, including the steps of bioauthenticating and determining whether a sub-credit limit is exceeded, to a "local" processor.

2. The words "local" or "locally" appear nowhere in the claim.

3. According to the claim, the "consumer electronics device" *comprises* a "processor," but the claim does not state where the processor is located or where its functions must be performed.

4. Although a "consumer electronics device" may be a single, unitary object, housing all the functions needed to operate the device, that is not always the case. Consumer electronics devices packaged to include, for example, a combination of a base station and a remote transmitter, whereby the base station processes information received from the remote transmitter (e.g., by wireless communication), are also well known.

5. Claim 5 is worded broadly and thus does not exclude such a combination.

6. Furthermore, the Specification describes, as an embodiment of the inventive device, a system wherein the bioauthentication and sub-credit limit matching functions reside on a server:

> It is another object of the invention to provide a method and device, which, based on authentication of the user, enables the owner of the account to easily delegate different monetary degrees of access to the owner's single account to different people and enables the entire family to access the account via a bioauthentication sensor. In this embodiment the account and bioauthentication information is stored at a server so that access to the server can be achieved at home, at school, in a hotel, or other remote location.

(Specification 2:20-3:4.)

7. The Specification further describes using the server as the processor:

> An authorized user then uses his PC, mobile phone or television 10 to access the Internet and an on-line store 11. The authorized user selects an item or service for purchase. The on-line store 11 requests a credit card number. The bioauthentication information (fingerprint, iris scan etc.) is sent to the server 12. The server 12 locates the correct credit card information and checks whether the authorized user can spend the amount requested. In one embodiment, the authorized user informs the server 12 of the amount to be spent and in another embodiment the on-line store 11 gives the amount to the server. If authorization is approved, the server 12 sends the on-line store 11 the credit card information required to complete the sale.

(Specification 6:3-13.)

8. Because the scope of claim 5 is not limited to use of a "local" processor, Nakano discloses all of the elements of claim 5 except for Nakano's authentication information is not provided by a bioauthentication device (Answer 3-5) (Appeal Br. 8-9).

9. The Examiner found that Harada discloses "bio-authentication information as the identification information where [the] bio-authentication device provides the bio-authentication information that is a fingerprint (col 7, lines 19-23) further where the sensor is on the remote control (col 7, lines 14-18)" (Answer 6). Appellant did not traverse these findings by the Examiner as to the scope and content of Harada (Appeal Br. 10-

11 and 17-18). Thus, Harada shows that the use of a bioauthentication device (fingerprint sensor) on a consumer electronics device (remote control) to provide bioauthentication information (fingerprint) was known in the prior art at the time of the invention.

10. Harada teaches to use bioauthentication information, such as a voice print or fingerprint, "to prevent unauthorized tampering with [certain terminal setting] data by persons who may have access to the remote control apparatus" (Harada, col. 4, ll. 32-34), "to ensure that the type of service which is provided by a terminal apparatus to the users of its remote control apparatuses is selectively controlled in accordance with various different categories of uses, e.g.[,] adults and children" (Harada, col. 4, ll. 56-60), and "to reliably ensure that certain services which should be available only to a specific individual user ... and which can be requested by operation of a remote control apparatus, will in fact be made available only to the appropriate individual, when a number of different individuals can use remote control apparatus to communicate with that same terminal apparatus" (Harada, col. 4, l. 61 – col. 5, l. 3).

11. What is clear from Harada is that the use of a PIN code is not as reliable an identifier as bioauthentication information because the PIN can be stolen and used without the authorized user's knowledge by anyone who may have access to the remote control apparatus.

12. Harada suggests that bioauthentication information, such as a fingerprint, unambiguously and reliably ensures that a specific authorized user is requesting the service.

13. We further note that use of a PIN code as an identifier is not as desirable as bioauthentication information because the use of a PIN requires the user to remember the PIN code.

14. Dethloff is directed to "plastic devices, comprising integrated circuits, commonly called 'smart cards'" (Dethloff, col. 1, ll. 12-18).

15. Dethloff is specifically directed to modules or "M-cards" which comprise a keyboard for entering, for example, identification and transaction data, a memory for storing data, a logic means, and a display (Dethloff, col. 9, ll. 57-68).

16. Dethloff's M-card contains means to assign the card to a number of sub-users (Dethloff, col. 5, ll. 19-20), each of which can be designated a particular value (Dethloff, col. 5, ll. 20-28). This is accomplished by the card-holder assigning each sub-user a PIN and a transaction limit (see, e.g., Dethloff, col. 6, ll. 64- col. 7, l. 4; Fig. 9), which are stored in a memory means in the card (PIN: Dethloff, col. 11, l. 10; transaction limit: Dethloff, col. 13, ll. 17-21).

17. In operation, a sub-user will authenticate the M-card by inputting a PIN which the card then internally checks for correctness (Dethloff, col. 10, ll. 63-67; see also col. 13, ll. 35-38). This then triggers a means within the card to open a transaction account assigned to the sub-user (Dethloff, col. 12,

ll. 62-64) permitting the sub-user to conduct transactions up to the maximum sub-user transaction amount (Dethloff, col. 13, ll. 19-21).

18. Dethloff states that instead of a PIN, a voice print (a type of bioauthentication) may be used as the sub-user enabling code:

> It is noted that while the PIN is given as an example of cardholder and sub-user enabling code, any other code can be used, such as a voice print (to be stored as data and input by the cardholder or sub-user) . . .

(Dethloff, col. 11, ll. 26-29.) Thus, Dethloff explicitly shows that the substitution of alternative user authentication techniques is known in the prior art. In particular, Dethloff teaches that it was known in the art at the time of the invention to substitute a PIN authentication with bioauthentication to enable a user to access credit.

19. The art of consumer electronics devices evidences a common usage of personal codes or personal identification numbers (PINs) to identify or authenticate users (e.g., Nakano, col. 4, ll. 42-45 and col. 5, ll. 39-42 and Dethloff, col. 10, ll. 59-67).

20. The art further shows that one of ordinary skill in the consumer electronic device art at the time of the invention would have been familiar with using bioauthentication information interchangeably with or in lieu of PINs to authenticate users (Harada, col. 7, ll. 14-23 and Dethloff, col. 11, ll. 26-29.)

21. It is also clear from an examination of the prior art that those of ordinary skill in the consumer electronic device art at the time

of the invention were familiar with the use of bioauthentication devices to obtain bioauthentication information to identify users (Harada, col. 7, ll. 14-23).

PRINCIPLES OF LAW

"Section 103 forbids issuance of a patent when 'the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains.'" *KSR Int'l Co. v. Teleflex Inc.*, 127 S.Ct. 1727, 1734, 82 USPQ2d 1385, 1391 (2007). The question of obviousness is resolved on the basis of underlying factual determinations including (1) the scope and content of the prior art, (2) any differences between the claimed subject matter and the prior art, (3) the level of skill in the art. *Graham v. John Deere Co.*, 383 U.S. 1, 17-18, 148 USPQ 459, 467 (1966). *See also KSR*, 127 S.Ct. at 1734, 82 USPQ2d at 1391 ("While the sequence of these questions might be reordered in any particular case, the [*Graham*] factors continue to define the inquiry that controls.") The Court in *Graham* further noted that evidence of secondary considerations, such as commercial success, long felt but unsolved needs, failure of others, etc., "might be utilized to give light to the circumstances surrounding the origin of the subject matter sought to be patented." 383 U.S. at 18, 148 USPQ at 467.

In *KSR*, the Supreme Court emphasized "the need for caution in granting a patent based on the combination of elements found in the prior art," *id.* at 1739, 82 USPQ2d at 1395, and discussed circumstances in which

a patent might be determined to be obvious without an explicit application of the teaching, suggestion, motivation test.

In particular, the Supreme Court emphasized that "the principles laid down in *Graham* reaffirmed the 'functional approach' of *Hotchkiss*, 11 How. 248." *KSR*, 127 S.Ct. at 1739, 82 USPQ2d at 1395 (citing *Graham v. John Deere Co.*, 383 U.S. 1, 12, 148 USPQ 459, 464 (1966) (emphasis added)), and reaffirmed principles based on its precedent that "[t]he combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results." *Id.* The Court explained:

> When a work is available in one field of endeavor, design incentives and other market forces can prompt variations of it, either in the same field or a different one. If a person of ordinary skill can implement a predictable variation, §103 likely bars its patentability. For the same reason, if a technique has been used to improve one device, and a person of ordinary skill in the art would recognize that it would improve similar devices in the same way, using the technique is obvious unless its actual application is beyond his or her skill.

Id. at 1740, 82 USPQ2d at 1396. The operative question in this "functional approach" is thus "whether the improvement is more than the predictable use of prior art elements according to their established functions." *Id.*

The Supreme Court made clear that "[f]ollowing these principles may be more difficult in other cases than it is here because the claimed subject matter may involve more than the simple substitution of one known element for another or the mere application of a known technique to a piece of prior art ready for the improvement." *Id.* The Court explained, "[o]ften, it will be

necessary for a court to look to interrelated teachings of multiple patents; the effects of demands known to the design community or present in the marketplace; and the background knowledge possessed by a person having ordinary skill in the art, all in order to determine whether there was an apparent reason to combine the known elements in the fashion claimed by the patent at issue." *Id.* at 1740-41, 82 USPQ2d at 1396. The Court noted that "[t]o facilitate review, this analysis should be made explicit. *Id.* (citing *In re Kahn,* 441 F.3d 977, 988, 78 USPQ2d 1329, 1336 (Fed. Cir. 2006)) ("[R]ejections on obviousness grounds cannot be sustained by mere conclusory statements; instead, there must be some articulated reasoning with some rational underpinning to support the legal conclusion of obviousness"). However, "the analysis need not seek out precise teachings directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." *Id.* at 1741, 82 USPQ2d at 1396.

The Supreme Court's opinion in *United States v. Adams*, 383 U.S. 39, 40, 148 USPQ 479, 480 (1966) is illustrative of the "functional approach" to be taken in cases where the claimed invention is a prior art structure altered by substituting one element in the structure for another known element. *KSR*, 127 S.Ct. at 1734, 82 USPQ2d at 1391. "The Court [in *Adams*] recognized that when a patent claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result. 383 U.S., at 50-51." *Id.* Ultimately the *Adams* Court found the combination at issue *not* obvious to those skilled in the art because, although the elements were known in the prior art, they worked together in an *unexpected* manner.

> The [*Adams*] Court relied upon the corollary principle that when the prior art teaches away from combining certain known elements, discovery of a successful means of combining them is more likely to be nonobvious. *Id.*, at 51-52, 86 S.Ct. 708. When Adams designed his battery, the prior art warned that risks were involved in using the types of electrodes he employed. *The fact that the elements worked together in an unexpected and fruitful manner supported the conclusion that Adams's design was not obvious to those skilled in the art.*

KSR, 127 S.Ct. at 1740, 82 USPQ2d at 1395 (emphasis added).

The Federal Circuit recently concluded that it would have been obvious to combine (1) a mechanical device for actuating a phonograph to play back sounds associated with a letter in a word on a puzzle piece with (2) an electronic, processor-driven device capable of playing the sound associated with a first letter of a word in a book. *Leapfrog Ent., Inc. v. Fisher-Price, Inc.*, 485 F.3d 1157, 1161, 82 USPQ2d 1687, 1690-91 (Fed. Cir. 2007) ("[a]ccommodating a prior art mechanical device that accomplishes [a desired] goal to modern electronics would have been reasonably obvious to one of ordinary skill in designing children's learning devices"). In reaching that conclusion, the Federal Circuit recognized that "[a]n obviousness determine is not the result of a rigid formula disassociated from the consideration of the facts of a case. Indeed, the common sense of those skilled in the art demonstrates why some combinations would have been obvious where others would not." *Id.* at 1161, 82 USPQ2d at 1687 (citing *KSR*, 127 S.Ct. 1727, 1739, 82 USPQ2d 1385, 1395 (2007) ("The combination of familiar elements according to known methods is likely to be obvious when it does no more than yield predictable results."). The Federal Circuit relied in part on the fact that Leapfrog had presented no evidence that the inclusion of a reader in the combined device was "uniquely challenging

or difficult for one of ordinary skill in the art" or "represented an unobvious step over the prior art." *Id.* (citing *KSR*, 127 S.Ct. at 1740-41, 82 USPQ2d at 1396).

The person of ordinary skill in the art is a hypothetical person who is presumed to know the relevant prior art. *Custom Accessories, Inc. v. Jeffrey-Allan Indus., Inc.*, 807 F.2d 955, 962, 1 USPQ2d 1196, 1201 (Fed. Cir. 1986). In determining this skill level, the court may consider various factors including "type of problems encountered in the art; prior art solutions to those problems; rapidity with which innovations are made; sophistication of the technology; and educational level of active workers in the field." *Id.* (*cited in In re GPAC*, 57 F.3d 1573, 1579, 35 USPQ2d 1116, 1121 (Fed. Cir. 1995)). In a given case, every factor may not be present, and one or more factors may predominate. *Id.* at 962-63, 1 USPQ2d at 1201.

ANALYSIS

Claim Interpretation

Appellant argues that claim 5 should be limited to a "local" processor. Claims are given their broadest reasonable construction "in light of the specification as it would be interpreted by one of ordinary skill in the art." *In re Am. Acad. of Sci. Tech. Ctr.*, 367 F.3d 1359, 1364, 70 USPQ2d 1827, 1830 (Fed. Cir. 2004). Claim 5 does not describe the device in terms that limit any function, including the steps of bioauthenticating and determining whether a sub-credit limit is exceeded, to a "local" processor (FF 1). In fact, the words "local" or "locally" appear nowhere in the claim (FF 2). The only recitation in the claim relevant to the question of where the processor and its recited functions may be located in the claimed device is in the preamble,

i.e., in the phrase "consumer electronics device" itself. According to the claim, the "consumer electronics device" *comprises* a "processor" but it does not say where the processor is located or where its functions must be performed (FF 3). Although a "consumer electronics device" may be a single, unitary object, housing all the functions needed to operate the device, that is not always the case. Consumer electronics devices packaged to include, for example, a combination of a base station and a remote transmitter whereby the base station processes information received from the remote transmitter (e.g., by wireless communication) are also well known (FF 4). The claim is worded broadly and thus does not exclude such a combination (FF 5). Furthermore, the Specification describes, as an embodiment of the inventive device, a system wherein the bioauthentication and sub-credit limit matching functions reside on a server (FF 6, 7). In light of the Specification, the claimed "device" has a broad scope and does not limit the processor to one that is "locally" positioned.

The Graham Factors

The patentability of claim 5 under 35 U.S.C. § 103(a) (2002) depends on whether the claimed subject matter is obvious in view of Nakano, Dethloff, and Harada.

The Examiner found that Nakano discloses all of the elements of claim 5 except for Nakano's authentication information is not provided by a bioauthentication device, and Nakano fails to disclose a local storage device for the memory, where the memory is part of the consumer electronics device (Answer 4-5). The Appellant does not traverse these findings by the Examiner (Appeal Br. 8-9). We disagree, however, with the Examiner's

implied finding that claim 5 requires the memory to be stored in a local storage device, as discussed *supra*. Accordingly, we disagree with Appellant's argument that the claimed device distinguishes over Nakano because Nakano determines whether a sub-credit limit is exceeded at a remote server rather than "locally." Thus, the sole difference between Nakano and the subject matter of claim 5 is that Nakano does not disclose the authentication information being provided by a bioauthentication device (FF 8).

The Examiner found that Harada discloses "bio-authentication information as the identification information where [the] bio-authentication device provides the bio-authentication information that is a fingerprint (col 7, lines 19-23) further where the sensor is on the remote control (col 7, lines 14-18)" (Answer 6). Appellant did not traverse these findings by the Examiner as to the scope and content of Harada (Appeal Br. 10-11 and 17-18). Thus, Harada shows that the use of a bioauthentication device (fingerprint sensor) on a consumer electronics device (remote control) to provide bioauthentication information (fingerprint) was known in the prior art at the time of the invention (FF 9).

Because Nakano teaches every element of the device of claim 5 but for the bioauthentication device element, the sole difference between Appellant's claim 5 and the teachings of Nakano is the use of bioauthentication in place of Nakano's password authentication (FF 8). In that regard, Harada shows that it was known in the art at the time of the invention to use a bioauthentication device on a remote control to provide the bioauthentication information (FF 9).

With regard to Dethloff, the Examiner found:

> Dethloff et al discloses bio-authentication information as the identification information further as a voice sensor (col 11, lines 25-30), a local storage device for the memory further where the memory is part of the consumer electronics device (col 11, lines 2-24), sending account holder information over the communication link, a match detected and determining a sub-credit limit that is not exceeded (col 13, lines 67-68; col 14, lines 1-8).

(Answer 5.) We agree with the Examiner that Dethloff discloses that instead of using a PIN for authentication, a voice print (a type of bioauthentication) may be used as the sub-user enabling code (FF 18). As such, Dethloff teaches that it was known in the art at the time of the invention to substitute a PIN authentication with bioauthentication to enable a user to access credit via a consumer electronics device (FF 18).

We find, based on our examination of the prior art and the state of the art in consumer electronic devices, that the art evidences a common usage of personal codes or personal identification numbers (PINs) to identify or authenticate users (FF 19). The art further shows that one of ordinary skill in the consumer electronic device art at the time of the invention would have been familiar with using bioauthentication information interchangeably with or in lieu of PINs to authenticate users (FF 20). It is also clear from an examination of the prior art that those of ordinary skill in the consumer electronic device art at the time of the invention would have been familiar with using bioauthentication devices to obtain bioauthentication information to identify users (FF 21).

Obviousness

Based on an analysis of the scope and content of Nakano and Harada, the facts support the conclusion that, but for the bioauthentication means, Nakano discloses all the elements of the claimed device and their functions and that the bioauthentication means was disclosed in Harada. Since each individual element and its function, as described in claim 5, are shown in the prior art, albeit shown in separate references, the difference between the claimed subject matter and that of the prior art rests not on any individual element or function but in the very combination itself; that is, in the substitution of Harada's bioauthentication device for Nakano's manual authentication means. Where, as here "[an application] claims a structure already known in the prior art that is altered by the mere substitution of one element for another known in the field, the combination must do more than yield a predictable result," *KSR*, 127 S.Ct. at 1740, 82 USPQ2d at 1395 (citing *United States v. Adams*, 383 U.S. 50-51, 148 USPQ 479, 483 (1966)). In that regard, Appellant has provided no evidence that replacing Nakano's manual authentication means with Harada's known bioauthentication means yields an unexpected result or was beyond the skill of one having ordinary skill in the art.

The Appellant's own Specification only generally describes the idea of incorporating a bioauthentication device, such as a fingerprint sensor, into a consumer electronics device and the matching function needed to compare the scanned bioauthentication information with the stored bioauthentication information (e.g., Specification 6:6-7 and 6:17-7:2). The Specification does not provide a detailed description of the implementation in hardware or software of the bioauthentication device. Furthermore, Appellant's Specification as well as Appellant's arguments do not present any evidence

that including the bioauthentication device into the consumer electronic device was uniquely challenging or difficult for one of ordinary skill in the art.

As in *Leapfrog*, the device defined by claim 5 is an adaptation of an old invention (Nakano) using newer technology that is commonly available and understood in the art (Harada). Adding bioauthentication to the Nakano device does no more to Nakano's device than it would do if it were added to any other device. The function remains the same. Predictably, bioauthentication adds greater security and reliability to an authorization process (FF 12). This variation on Nakano's device, whereby the manual authentication means of the Nakano device is replaced with Harada's bioauthentication means, appears to present no unexpected technological advance in the art. One of ordinary skill in the art of consumer electronic devices would have found it obvious to update the Nakano device with the modern authentication components of the Harada bioauthentication means and thereby gaining, predictably, the commonly understood benefits of such adaptation, that is, a secure and reliable authentication procedure (FF 12).

Appellant argues that the Examiner has failed to provide sufficient reasoning to reach a conclusion of obviousness based on the prior art (Appeal Br. 11-20). Appellant repeatedly argues for application of the teaching, suggestion, motivation (TSM) test, stating that "[t]here must be some suggestion or motivation, either in the references themselves, or in the knowledge generally available to one of ordinary skill in the art, to modify a reference or to combine reference teachings" (e.g., Appeal Br. 11). The Supreme Court noted in *KSR* that although the TSM test "captured a helpful insight," an obviousness analysis "need not seek out precise teachings

directed to the specific subject matter of the challenged claim, for a court can take account of the inferences and creative steps that a person of ordinary skill in the art would employ." 127 S.Ct. at 1741, 82 USPQ2d at 1396.

The claim is to a structure already known in the prior art that is altered by the mere substitution of one known element for another element known in the field for the same function. The facts themselves show that there is no difference between the claimed subject matter and the prior art but for the combination itself. "[T]he mere existence of differences between the prior art and an invention does not establish the invention's nonobviousness. The gap between the prior art and respondent's system is simply not so great as to render the system nonobvious to one reasonably skilled in the art." *Dann v. Johnston*, 425 U.S. 219, 230, 189 USPQ 257, 261 (1976) (holding that claims directed to a machine system for automatic record keeping of bank checks and deposits were obvious in view of the use of data processing equipment and computer programs in the banking industry at the time of the invention in combination with a prior art automatic data processing system using a programmed digital computer for use in a large business organization). Appellant has presented no evidence that combining the Nakano device with the Harada bioauthentication means would have required anything more from one of ordinary skill in the art than to substitute one authentication means for a more advanced one. Accordingly, we hold that the subject matter of claim 5 would have been obvious to one of ordinary skill in the art given the teachings of Nakano and Harada.

Nonetheless, our holding is further buttressed by the teaching in Dethoff of the substitutability of a voice print authentication for a PIN authentication (FF 10). In particular, Dethloff teaches that it was known in

the art at the time of the invention to substitute a PIN authentication with bioauthentication to enable a user to access credit (FF 10, 20).

Further, Harada provides sufficient motivation for one skilled in the art to use this bioauthentication information, such as a voice print or fingerprint, in lieu of a PIN in order "to prevent unauthorized tampering with [certain terminal setting] data by persons who may have access to the remote control apparatus," "to ensure that the type of service which is provided by a terminal apparatus to the users of its remote control apparatuses is selectively controlled in accordance with various different categories of uses, e.g.[,] adults and children," and "to reliably ensure that certain services which should be available only to a specific individual user ... and which can be requested by operation of a remote control apparatus, will in fact be made available only to the appropriate individual, when a number of different individuals can use remote control apparatus to communicate with that same terminal apparatus" (FF 10). The use of a PIN code is not as reliable an identifier as bioauthentication information because the PIN can be stolen and used without the authorized user's knowledge (FF 11). On the contrary, bioauthentication information, such as a fingerprint, unambiguously and reliably ensures that a specific authorized user is requesting the service (FF12). Further, use of a PIN code as an identifier is not as desirable as bioauthentication information because the use of a PIN requires the user to remember the PIN code (FF 13).

Thus, one of ordinary skill in the art would have been motivated to combine the bioauthentication device of Harada with the system of Nakano because Dethloff teaches that one can substitute bioauthentication information for PIN information, and Harada teaches that it was a common

problem at the time of the invention to create a remote control that would reliably ensure that the appropriate person was given access to the system. The use of a fingerprint scanner, such as disclosed in Harada, was an obvious solution to provide a more reliable means of identification than the PIN code of Nakano. *KSR*, 127 S.Ct. at 1742, 82 USPQ2d at 1397 ("[o]ne of the ways in which a patent's subject matter can be proved obvious is by noting that there existed at the time of invention a known problem for which there was an obvious solution encompassed by the patent's claims.") As such, we sustain the Examiner's rejection of claims 5-11 and 13-16 as unpatentable over Nakano, Harada, and Dethloff.

CONCLUSION OF LAW

On the record before us, Appellant has failed to show that the Examiner erred in rejecting the claims over the prior art.

DECISION

The decision of the Examiner to reject of claims 5-11 and 13-16 under 35 U.S.C. § 103(a) as obvious over Nakano, Harada, and Dethloff is affirmed.

No time period for taking any subsequent action in connection with this appeal may be extended under 37 C.F.R. § 1.136(a)(1)(iv).

AFFIRMED

hh

PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510